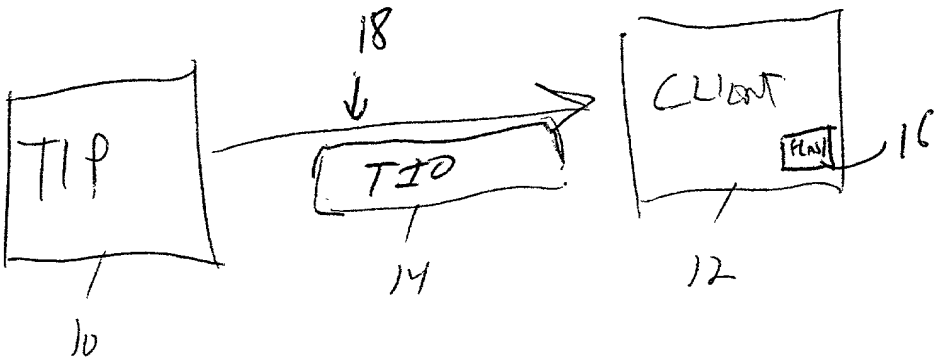

Fig. 1

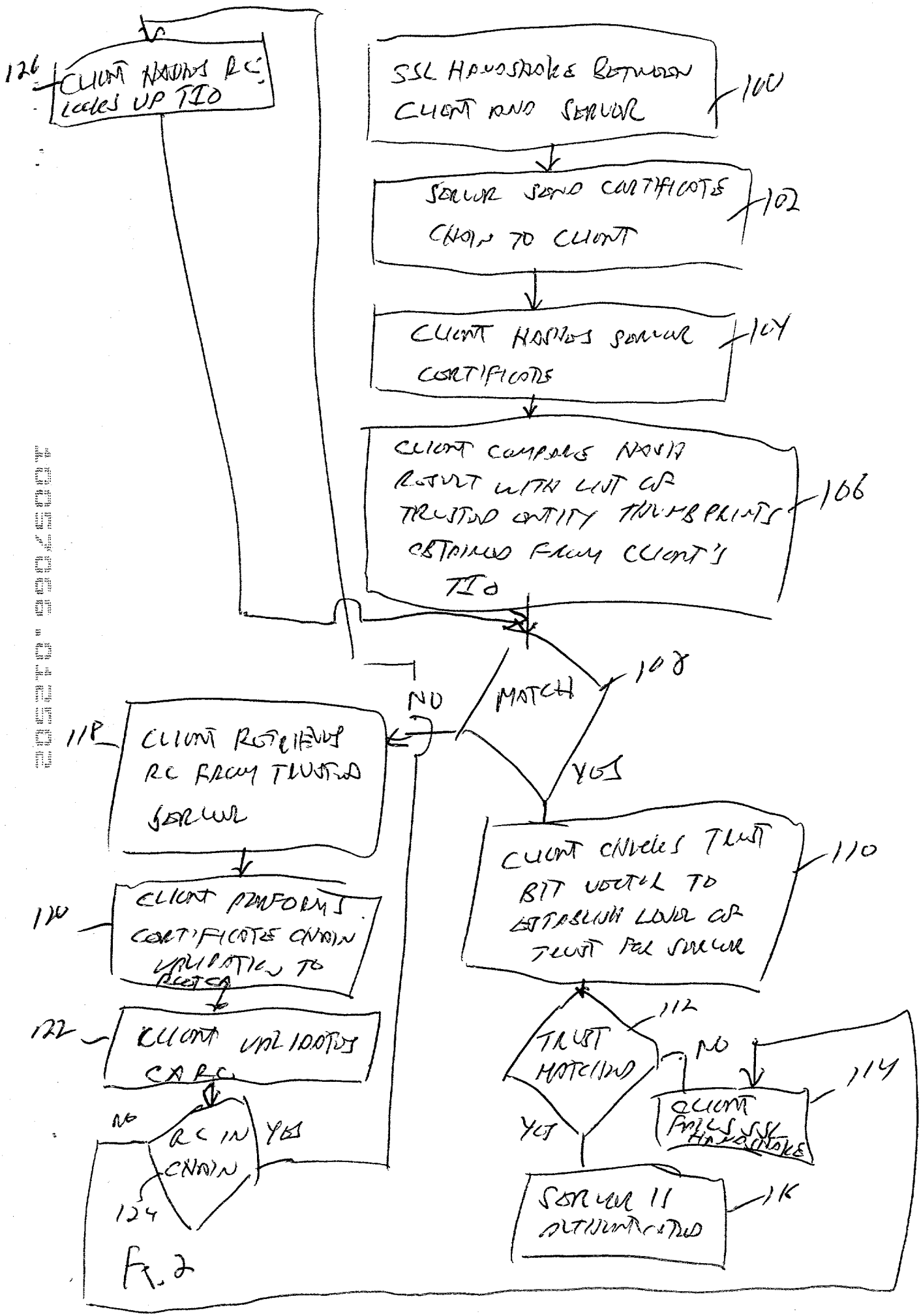
126
CLIENT KNOWS RC; LOOKS UP TIO
SSL HANDSHAKE BETWEEN CLIENT AND SERVER
100
SERVER SENDS CERTIFICATE CHAIN TO CLIENT
102
CLIENT HASHES SERVER CERTIFICATE
104
CLIENT COMPARES HASH RESULT WITH LIST OF TRUSTED ENTITY THUMBPRINTS OBTAINED FROM CLIENT'S TIO
106
MATCH
108
NO
YES
118
CLIENT RETRIEVES RC FROM TRUSTED SERVER
CLIENT CHECKS TRUST BIT VECTOR TO ESTABLISH LEVEL OF TRUST FOR SERVER
110
120
CLIENT PERFORMS CERTIFICATE CHAIN VALIDATION TO ROOT CA
122
CLIENT VALIDATES CA RC
RC IN CHAIN
NO
YES
124
TRUST MATCHING
112
NO
YES
CLIENT FAILS SSL HANDSHAKE
114
SERVER IS AUTHENTICATED
116

Fig. 2

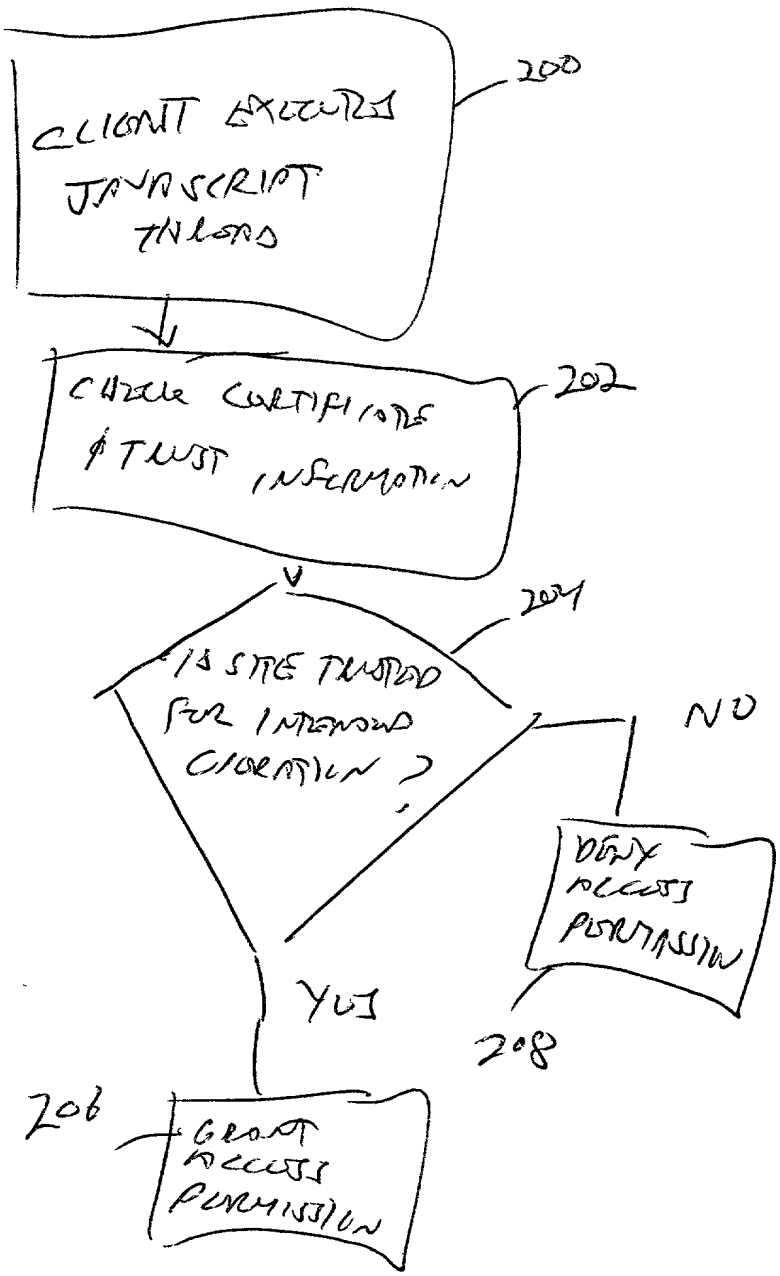
CLIENT EXECUTES JAVASCRIPT PAYLOAD
200
CHECK CERTIFICATE & TRUST INFORMATION
202
IS SITE TRUSTED FOR INTENDED OPERATION?
204
NO
DENY ACCESS PERMISSION
208
YES
206
GRANT ACCESS PERMISSION

Fig 3

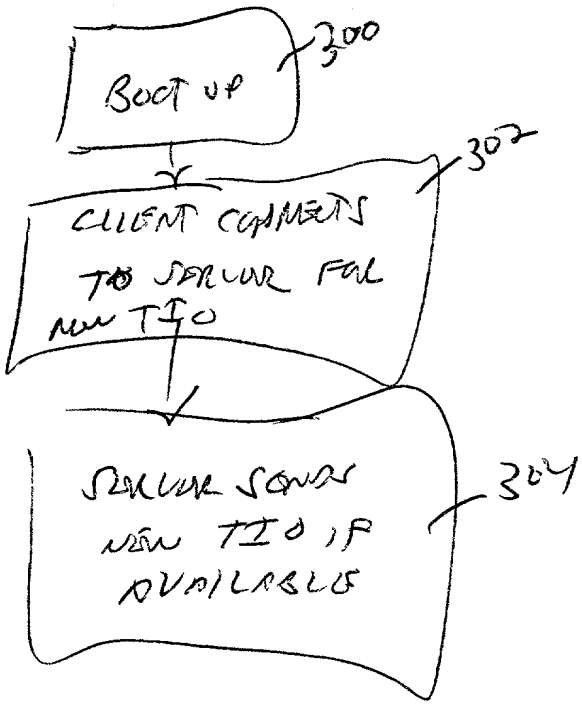
BOOT UP
300
CLIENT CONNECTS TO SERVER FOR NEW TIO
302
SERVER SENDS NEW TIO IF AVAILABLE
304

Fig 4

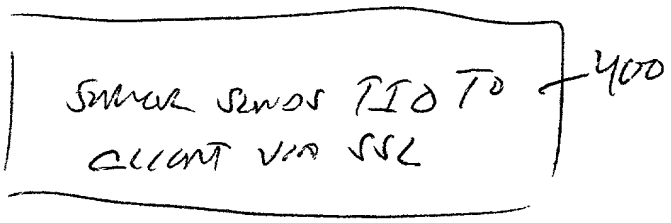

Fig. 5

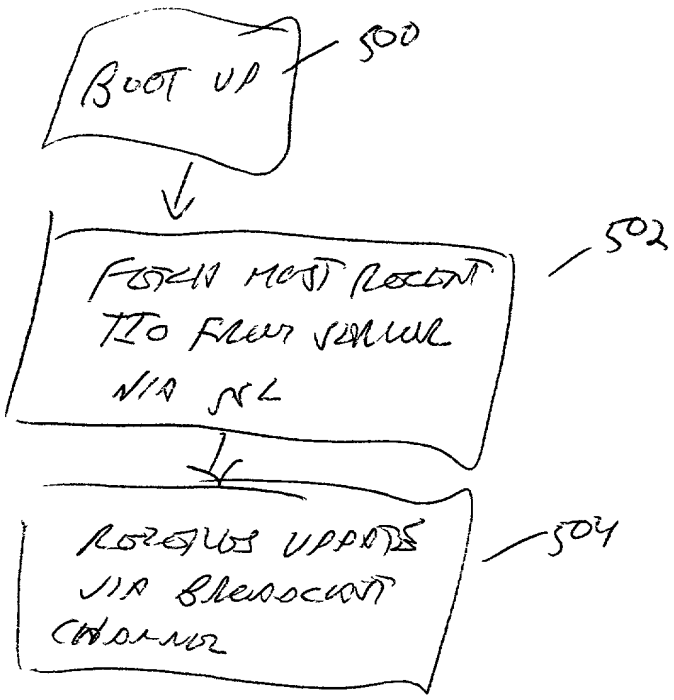
BOOT UP
500
FETCH MOST RECENT TLO FROM SERVER VIA NL
502
RECEIVE UPDATE VIA BROADCAST CHANNEL
504

Fig. 6